Information Processing

コンピュータ セキュリティ

真にパーソナルなコンピュータであれば、使用者の不注意あるいは事故などによる他は、重要なプログラムやデータが消去されてしまったり、改変されているなどというようなことはまず起こりえないわけである。しかしながらコンピュータシステムを複数の利用者が使用するような形態をとる場合、ことにそれが不特定多数であるような場合には、悪意のあるなしは別として、そういう事態が発生する可能性が生ずることになる。

この分野の先進国である合衆国の場合はこの問題は非常に深刻である。もちろん合衆国の場合はこの手のものにかぎらず、犯罪の発生率は高い訳であるから国民のモラルの水準が低いせいだと考えることもできる。（かの知的水準の低い中曽根首相と同じ様なことを言うな　と、叱られるかもしれませんが）しかし、我が国のモラルもそれほど高いとも思われない。したがってこの手の犯罪（犯罪にならぬ程度のものも含めて）が我が国でも多発する恐れは充分ある。つい先日もトリスタン計画のコンピュータがハッカーによって不正使用されるという事件が発生している。（報道によれば、日本人の仕業ではないようであるが）あるいは某大学の計算機センターのプログラムやデータが何者かによって消去されてしまうという事件も起こっている。また、キャッシュカード偽造事件や、失業保険金搾取事件等等さまざまな事態が発生している。

ところで、これらのコンピュータにかかわる犯罪はおおまかに言って二通りに分けることができる。一つはハッカーに代表されるようなコンピュータ侵入事件であり、もう一つはキャッシュカード偽造事件のような内部の人間による犯罪である。

コンピュータ侵入事件は、すべてのコンピュータシステムで起き得るといった性格のものではない。通信回線によって端末装置が結合されているオンラインシステムでのみ起こり得るのである。したがって、外部との接触を行わない閉じたシステムである場合にはこのような事態は発生しない訳である。また、オンラインシステムであっても、専用回線を使用する場合は安全である。オンラインで、なおかつ公衆回線によるサービスをおこなっているシステムでのみ起こり得るのである。したがって侵入事件は大学や研究所の計算機センター等で発生することが多いのである。この場合の防御策としては、利用者のパスワードを知られにくくするという事があげられるが、それだけでは防ぎ切れるものではないので、侵入されても重要な部分には影響が及ばないように配慮することが必要である。

一方、内部の人間に依る犯罪はあらゆるコンピュータシステムで発生する。そのシステムの内部事情を熟知する者がそれを悪用する場合には、どのような防御策も無駄である。したがってこの場合には、そういう気にさせないような環境を作りながら、コンピュータに携わる人間のモラルの向上に努めることが必要になってくる。